Michael Critchley
Amy Luria
CRITCHLEY, KINUM & LURIA, LLC
75 Livingston Avenue
Roseland, New Jersey 07068
Tel. (973) 422-9200
mcritchley@critchleylaw.com
aluria@critchleylaw.com

Steig D. Olson
Patrick D. Curran
David S. Mader
David LeRay
Matthew Fox
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, New York 10010
Tel. (212) 849-7000
steigolson@quinnemanuel.com

Michelle Schmit
QUINN EMANUEL URQUHART & SULLIVAN, LLP
191 N. Wacker Drive, Suite 2700
Chicago, Illinois 60606
Tel. (312) 705-7400
michelleschmit@quinnemanuel.com

Attorneys for Plaintiffs-Counterclaim Defendants IQVIA Inc. and IMS Software Services, Ltd.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IQVIA INC. and IMS SOFTWARE SERVICES, LTD.,

Plaintiffs – Counterclaim Defendants,

v.

VEEVA SYSTEMS, INC.,

Defendant – Counterclaim Plaintiff.

Case No.: 2:17-cv-00177-JXN-JSA

Hon. Julien Xavier Neals
Hon. Jessica S. Allen, U.S.M.J.
Hon. Dennis M. Cavanaugh, Ret. U.S.D.J.

[TO BE FILED UNDER SEAL]

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT ON PLAINTIFFS' TRADE SECRET CLAIMS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Other Authorities

PRELIMINARY STATEMENT

Plaintiffs IQVIA Inc. and IMS Software Services, Ltd. (collectively, "IQVIA") respectfully move for partial summary judgment on two issues: (1) that IQVIA's proprietary compilations of healthcare information, offered and licensed to clients in the U.S. under the brand names OneKey, DDD, and Xponent, qualify for trade secret protection under federal and state law and (2) that Defendant Veeva Systems, Inc. ("Veeva") misappropriated those compilations by, among other things, improperly acquiring and using them to build its own competing offering, Veeva OpenData. After years of discovery, the core facts that support these findings are clear and indisputable.

Veeva has spent the last seven years trying to complicate and confuse the issues—but at bottom, this case is simple and straightforward. IQVIA has built three industry-leading compilations of healthcare information through decades of market research, data acquisition and analysis, and massive investments. In 2013, envious of IQVIA's success, Veeva decided it wanted its own healthcare data offering. But Veeva, a Silicon Valley software company that prides itself on moving quickly, did not have experience with building these types of offerings, the patience to build them through independent research, or the willingness to invest the significant time and money it takes to build high-quality market research offerings like IQVIA's. Nevertheless, Veeva rashly announced it was entering the market with its own offering (Veeva OpenData) before it had even figured out a viable plan to develop one.

Having no honest path to build overnight what it had taken IQVIA decades (and hundreds of millions of dollars) to build, Veeva resorted to theft. As detailed below, Veeva bought a cheap, low-quality healthcare dataset from another company (AdvantageMS) and then proceeded to ***use IQVIA's offerings*** to turn that low-quality dataset into a commercially viable one. Through years of rampant misappropriation from IQVIA, Veeva took an unlawful shortcut to success.

There are no real factual disputes about any of this. Years of discovery confirm Veeva's misconduct. Resolving undisputed issues now will streamline this case for trial. Accordingly, the Court should enter partial summary judgment on the following two issues:

First, the Court should find that three of IQVIA's proprietary compilations of healthcare information—OneKey, DDD, and Xponent—qualify for trade secret protection under federal and state law. The Defend Trade Secrets Act, 18 U.S.C. § 1836(b) ("DTSA"), broadly defines a trade secret as "all forms and types of financial, business, scientific, technical, economic, or engineering information," including "***compilations***," when "the owner thereof has taken reasonable measures to keep such information secret," and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by[] another . . ." 18 U.S.C. § 1839(3) (emphasis added). As discussed below, the applicable state law, the New Jersey Trade Secrets Act, mirrors the DTSA in this regard.

There can be no dispute that IQVIA takes reasonable measures to keep OneKey, DDD, and Xponent secret, nor that IQVIA derives ***actual*** independent economic value from the confidentiality of these offerings, each of which IQVIA has built through decades of market research, data acquisition and analysis, and massive investments. IQVIA's clients pay millions of dollars to license each of these offerings from IQVIA year after year, demonstrating that these offerings provide economic value to IQVIA and that they are not readily ascertainable in the public domain. Moreover, IQVIA's clients pay these licensing fees because they know that is the ***only*** way they can access IQVIA's intellectual property, which is not available anywhere else because of the extensive and reasonable measures taken by IQVIA to protect the secrecy of its property.

Second, the Court should rule that Veeva misappropriated IQVIA's proprietary compilations through, among other things, the "improper acquisition" and the "use" of IQVIA's

compilations "without consent" to build its own competing offering (Veeva OpenData). *Oakwood Lab'ys LLC v. Thanoo*, 999 F.3d 892, 907–08 (3d Cir. 2021). There can be no reasonable dispute that Veeva engaged in the improper acquisition and unauthorized use of IQVIA's offerings as part of its efforts to build Veeva OpenData into a viable commercial offering quickly and on-the-cheap. As detailed below, and in IQVIA's Statement of Material Facts Not In Dispute Pursuant to Local Civil Rule 56.1 ("SOF") that accompanies this brief, Veeva's indisputable misappropriation of IQVIA's offerings took at least three forms.

1. Programmatic Theft from Data Feeds. Beginning in mid-2013, Veeva systematically fed IQVIA's offerings (which Veeva accessed through IQVIA's clients) into its "HDM" database where it used them to build Veeva OpenData. As noted, Veeva tried to jumpstart Veeva OpenData by buying AdvantageMS, a small company that did some basic data services work for several pharmaceutical companies, which included IQVIA's data clients. To perform some of this work, AdvantageMS maintained a basic, low-quality reference dataset that it kept in its internal database called "HDM." Because of its limited data services work on behalf of IQVIA's clients, AdvantageMS received a steady feed of IQVIA's proprietary data from certain mutual clients who licensed that data from IQVIA. After Veeva bought AdvantageMS in June 2013, Veeva had access to those same feeds of IQVIA's proprietary data. But instead of using that IQVIA data for the limited, authorized purpose of performing data services projects for IQVIA's clients, Veeva used that data for the clearly ***unauthorized*** purpose of building its competing data offering. Veeva made the reference data contained within HDM the foundation for Veeva OpenData and configured its systems to ***programmatically*** feed IQVIA's data into the HDM database. Veeva also put the entire set of IQVIA data it was receiving for limited data services projects into a series of tables for consumption by the very Veeva employees ("data

stewards") tasked with building Veeva OpenData, who could, as a result, improperly consult IQVIA's proprietary data to build out Veeva's competitive offering.

Veeva has since destroyed the underlying data feeds, tables, and other records that would have allowed IQVIA to show the granular details of Veeva's misappropriation regarding HDM. But, despite its efforts to cover its tracks, Veeva left a paper trail that lays out its misappropriation in Veeva's own words. For instance, the computer code that Veeva ran to destroy the tables containing evidence of its misuse of IQVIA's offerings still exists, and that code shows that Veeva had often given the tables of data that it used and then destroyed names that identify the IQVIA offerings that Veeva was improperly using (like "DDD" or "Xponent") right in the file name. In addition, an internal memo prepared by a Veeva executive in September 2015 (which Veeva had originally tried to hide under a baseless privilege claim that the Special Master and the Court both rejected) removes any possible ambiguity. This memo confirms that IQVIA's proprietary offerings were "***programmatically included within Veeva OpenData***," and that "***the entire set of IMS data is visible to Veeva OpenData stewards***."[1] This is a straightforward admission of Veeva's misappropriation. Indeed, this same memo concluded that, once IQVIA found out about the misappropriation, IQVIA "***will file a lawsuit against Veeva for damages***" for violating its intellectual property. The Court should, therefore, grant summary judgment on the issue that Veeva's unauthorized use of IQVIA data in programmatic data feeds and by Veeva OpenData data stewards was trade secret misappropriation.

2. Grading or Scoring IQVIA's Data. Beginning in late-2013, Veeva further engaged in rampant misuse of IQVIA's offerings under the guise of what it called a "Data Report Card" or "Scorecard" program. Here, Veeva went out to dozens of IQVIA's clients (without

[1] IQVIA is the successor entity to IMS Health (or "IMS").

telling IQVIA) and offered to give the data those clients licensed from IQVIA a free "report card" or a "score" compared to Veeva's data. And while Veeva has tried to portray this as an innocent marketing exercise, the very idea of Veeva grading IQVIA's data, especially at that time, is absurd. When Veeva launched this program, it had only recently purchased the cheap dataset from AdvantageMS, which Veeva's own executives recognized was of such low quality that it was not "commercially viable." Veeva was obviously in no position to use this low-quality dataset as a benchmark for grading IQVIA's high-quality, industry-leading data which IQVIA had been building over decades.

This would be like a lazy math student who never studies offering to "grade" or "score" the test of the best student in the class, before the tests are handed in. The real reason for the offer is obvious—the lazy student wants to compare his work against the best student's work in order to identify what the lazy student has done wrong. And that is exactly what Veeva did here. On at least ■ ***occasions***, Veeva improperly accessed IQVIA's proprietary offerings under the guise of giving IQVIA's clients a "report card" or "scorecard" and ran unauthorized comparisons of IQVIA's proprietary data. Once again, Veeva's own documents confirm this misappropriation and expressly state that Veeva used these unauthorized analyses of IQVIA's data to "***identify any potential gaps***" in Veeva OpenData and to figure out how to "***fill those gaps***."

Veeva tried to destroy the underlying records of this aspect of its misappropriation too. This Court has affirmed Judge Cavanaugh's finding that, ***after*** this litigation was filed, Veeva created a tracking spreadsheet (the "DataDestroyed Spreadsheet"), which recorded Veeva's then-ongoing efforts to track down and delete every extract of IQVIA's proprietary data that Veeva had analyzed as part of the program to prevent IQVIA from using those extracts to prove its case. Veeva has, incredibly, tried to weaponize this and other aspects of its spoliation, arguing that

IQVIA is somehow at fault because it cannot identify every single record that Veeva misused as part of the Data Report Card program, even though Veeva ***intentionally destroyed*** the extracts it improperly used as part of this program, in spoliation amounting to a crime and fraud on this Court. Veeva's efforts to benefit from its spoliation are completely improper and only confirm Veeva's awareness of its wrongdoing. The Court should grant summary judgment on the issue that Veeva misappropriated IQVIA's trade secrets through its Data Report Card program, by acquiring and using IQVIA data without permission, and by using that data to improve Veeva's offerings.

3. Soliciting IQVIA Data from Early Adopters. Starting in mid-2014, with its data still lagging well behind IQVIA's, Veeva convinced a few IQVIA clients to be "early adopters" of Veeva OpenData for rock-bottom prices. When these companies actually saw Veeva's data, however, they saw that it was poor quality and complained. Veeva then pressured them to send over their IQVIA data, which Veeva then improperly mined to build out Veeva OpenData even further. And while Veeva tried to cover up this misappropriation too, it was not able to destroy all of the evidence because many of the files of IQVIA's proprietary data that Veeva illicitly obtained and used were attached to emails that were produced in this litigation. IQVIA can, therefore, often show exactly what files and records Veeva improperly used and, in many cases, provide specific details about how Veeva used them. The Court should, therefore, also grant summary judgment on the issue that Veeva's requests for and receipt of IQVIA data from early adopters, without permission, as well as its use of that information to improve Veeva's products, were further acts of trade secret misappropriation.

In short, Veeva cannot seriously dispute that IQVIA's offerings warrant trade secret protection or that it engaged in misappropriation. Judge Cavanaugh previously found that "***Veeva was well aware that it was misappropriating IQVIA data***" and that, fearing a lawsuit, Veeva

destroyed an enormous amount of evidence to conceal the scope of the misappropriation that had indisputably occurred. Dkt. 349 (Sanctions Order) at 75 (emphasis added). These conclusions remain indisputable now. Clarifying that IQVIA's offerings warrant trade secret protection and that Veeva did, in fact, engage in misappropriation will greatly streamline trial. The jury can then focus on resolving any disputed questions about how much misappropriation occurred, and the damages Veeva owes IQVIA for its misappropriation. The Court should grant IQVIA's motion for partial summary judgment.

BACKGROUND

A. IQVIA's Proprietary Offerings

IQVIA has invested hundreds of millions of dollars, decades of time, and its unparalleled expertise into building one of the largest and most comprehensive collections of healthcare information in the world. SOF ¶¶ 68-72, 102-05; *see also* SOF ¶¶ 73-101 (detailing IQVIA's substantial investments to create and maintain OneKey); SOF ¶¶ 106-38 (detailing IQVIA's substantial investments to create and maintain Xponent and DDD). IQVIA's healthcare information enables pharmaceutical companies, medical researchers, and government agencies to accelerate their research, development, and provision of innovative medical treatments and therapies, in order to improve healthcare outcomes for patients. SOF ¶¶ 47-51; *see also* SOF ¶¶ 45-67 (explaining the value of OneKey, Xponent, and DDD to IQVIA's customers). Relevant here are three specific IQVIA offerings, which are IQVIA's intellectual property that it licenses to its clients for their internal use only. SOF ¶ 24.

1. IQVIA's OneKey Offering

IQVIA's OneKey offering is a highly accurate, continuously updated compilation of a host of market research, data, and information about healthcare professionals ("HCPs") (including physicians, physician assistants, nurses, and pharmacists) and healthcare organizations ("HCOs")

(including hospitals and nursing homes). SOF ¶¶ 30-38. OneKey is essentially a comprehensive reference guide containing virtually everything a life sciences company needs to know about the HCPs and HCOs operating within a particular geography and is therefore sometimes called "reference data."[2] OneKey provides searchable information for millions of HCPs and HCOs, with hundreds of fields of information or data points per HCP or HCO, including their demographic information, contact information, educational background, profession, medical specialties, licensing information, industry standard identifiers, nursing degree type, preferred communication channels, bed types, and affiliations between HCPs and HCOs, among other things. SOF ¶¶ 19, 33.

OneKey was launched in 1970 and IQVIA has continued to develop it in the decades since. SOF ¶ 68. IQVIA builds OneKey by sourcing data from thousands of different sources, in addition to conducting its own primary research. SOF ¶¶ 73-76. From there, IQVIA engages in extensive efforts to clean, merge, and organize the data it collects. IQVIA receives data files in different formats, which require standardizing; IQVIA must link and append incoming data to IQVIA's existing dataset (to avoid duplicating HCP or HCO records); and IQVIA must validate the accuracy of the incoming data, among many other things. SOF ¶¶ 77-79. IQVIA must also resolve discrepancies in incoming data and identify and rank the information that is most likely to be up-to-date and accurate. SOF ¶¶ 80-81. IQVIA accomplishes these objectives by deploying complex and sophisticated processes, including proprietary algorithms and decision rules, as well

[2] IQVIA's reference data is sometimes marketed under different brand names in other countries across the globe, but in the United States and Europe, IQVIA's reference data is branded as "OneKey." SOF ¶ 30. More formally, IQVIA often uses "Healthcare Professional and Organizational Data" to describe its reference data.

as manual processes, such as primary research. SOF ¶¶ 81-84. IQVIA's processes lead to hundreds of thousands of updates to OneKey each month in the United States alone. SOF ¶ 85.

IQVIA estimates that its OneKey offering is at least 98% accurate. SOF ¶ 99. This high degree of accuracy is highly valuable to IQVIA's clients, such as pharmaceutical companies, who rely on OneKey to ensure that doctors and hospitals are informed and educated so that the right medicines get to the right patients at the right time. SOF ¶ 47; *see also* SOF ¶¶ 53-66 (illustrating with an example the amount and quality of information that IQVIA's offerings provide on a given HCP).

2. IQVIA's DDD and Xponent Offerings

IQVIA's DDD and Xponent offerings provide authoritative, proprietary estimates of the sales of medicines and HCP prescribing activity, respectively, and are therefore sometimes referred to in the industry as "sales data" and "performance data." SOF ¶¶ 22, 39-44.[3] IQVIA's DDD offering is a compilation of information and estimates about sales volumes of prescription medications and over-the-counter products sold into retail (e.g., pharmacy) and non-retail (e.g., hospital) outlets. SOF ¶ 40. Xponent provides detailed information and estimates of the number of prescriptions written by HCPs for each medicine available in the U.S. SOF ¶ 41. For example, Xponent includes individual and aggregated data on physicians prescribing a particular medication, including their location and an estimate of the volume of their prescriptions. SOF ¶ 42. IQVIA's DDD and Xponent offerings include reference data and are infused with fields from IQVIA's OneKey offering as well, such as contact information for HCPs and HCOs. SOF ¶ 132.

[3] More formally, IQVIA sometimes uses the term "Sub-National Information" to describe sales and performance data.

DDD and Xponent cover sales and prescribing activity for over 100,000 pharmaceutical products. SOF ¶ 44. In the United States, IQVIA builds its DDD offering from sales data covering more than 50,000 stores (e.g., [redacted]) and 700 hospitals. SOF ¶ 114. IQVIA builds its Xponent offering from prescription data covering a broad sample of stores each week, including data on over 60 million prescriptions from over 36,000 retail, mail-order, and long-term care pharmacies. SOF ¶ 107; *see also* SOF ¶¶ 106-17 (detailing IQVIA's data sourcing for DDD and Xponent). For pharmacies for which IQVIA does not collect data, IQVIA uses statistical algorithms to estimate the number of prescriptions written by each HCP for each medication dispensed by that pharmacy. SOF ¶ 110.

IQVIA standardizes all this data using reference files, uses sophisticated and proprietary projection methodologies to estimate sales and prescribing activities based on statistically representative samples, and applies methodologies to impute data if, for example, information from a supplier or facility is interrupted. SOF ¶¶ 105, 126; *see also* SOF ¶¶ 118-28 (explaining IQVIA's methods for data processing and validation for DDD and Xponent). IQVIA's extensive efforts and quality-controls allow clients to rely on DDD and Xponent to equip their sales representatives with information about HCPs and HCOs to make their interactions with HCPs more efficient and productive. SOF ¶¶ 48-51.

3. IQVIA's Investments In Its Proprietary Offerings

IQVIA continuously makes large investments to maintain the high quality of OneKey, DDD, and Xponent, investing hundreds of millions of dollars to acquire data from thousands of sources. SOF ¶¶ 73-76 (data sourcing for OneKey); ¶¶ 103, 106-17 (data sourcing for DDD and Xponent). In 2015, IQVIA made another substantial investment by acquiring the OneKey offering in Europe from Cegedim, paying approximately $520 million to acquire it, along with tangential aspects of Cegedim's business. SOF ¶¶ 32, 71. IQVIA has also spent millions of dollars in labor

expenses to support the development of OneKey, DDD, and Xponent. SOF ¶¶ 69, 83, 104. IQVIA's OneKey group in the United States, for example, employs approximately 300 research associates and 50 technical analysts. SOF ¶ 83. This enables IQVIA to undertake over one hundred million quality-control checks on its DDD and Xponent offerings in the United States every week. SOF ¶¶ 109, 121-22.

IQVIA is able to invest so much in the quality of these offerings because IQVIA's clients pay substantial sums to license them. From 2013 to 2020, IQVIA earned [redacted] in licensing revenues from IQVIA's OneKey, DDD, and Xponent offerings. SOF ¶ 139-42. IQVIA's clients are willing to pay such substantial sums to license these offerings because they know the resulting data compilations are not available in the public domain.

4. IQVIA's Measures To Protect Its Proprietary Offerings

IQVIA engages in a host of measures to protect the economic value of its offerings. The reasonableness of these measures is demonstrated by the fact that IQVIA's clients pay IQVIA hundreds of millions of dollars for licenses to access the offerings, which they would not do if the same information was available in the public domain. IQVIA's ability to protect the intellectual property associated with its market research offerings facilitates IQVIA's continued investment in them. SOF ¶¶ 143-44.

IQVIA's protections are guided by a set of information security protections, which work in tandem as part of IQVIA's Integrated Information Security Framework. SOF ¶ 145. For example, IQVIA deploys [redacted] to protect its information internally within IQVIA: [redacted]. SOF ¶¶ 146-50. IQVIA classifies the information in IQVIA's OneKey, DDD, and Xponent offerings at Levels [redacted], with Level [redacted] restricting access to IQVIA employees on a "need to know" only basis, and Level [redacted] imposing additional restrictions. SOF

¶¶ 149-51. IQVIA uses data loss protection software to identify and monitor the transfer of any confidential information within or outside IQVIA's network. SOF ¶¶ 162-67. IQVIA requires employees to sign confidentiality agreements barring the disclosure of IQVIA's confidential information, including OneKey, DDD, and Xponent, and the confidential information of others, and requires employees to regularly attend information security training (with additional specific trainings for employees with access to IQVIA's OneKey, DDD, and Xponent offerings). SOF ¶¶ 168-79.

With respect to external measures, IQVIA provides its clients with access to OneKey, DDD, and Xponent only under licenses that are designed to preserve the confidentiality of IQVIA's offerings while also allowing customers to use IQVIA's market research offerings internally for their own commercial benefit. SOF ¶ 180; *see also* SOF ¶¶ 180-87 (detailing provisions in IQVIA's data license agreements with clients). IQVIA's data license agreements apply to both data licensed by IQVIA and derivations of this data. SOF ¶ 182. IQVIA's data license agreements contain a provision that prohibits the client from attempting to reverse engineer the data. SOF ¶ 184. IQVIA's data license agreements also prohibit clients from disclosing or providing to third parties any data, its contents, or any information or materials derived from it, as well as any other confidential information. SOF ¶ 187.

IQVIA's clients often request that IQVIA grant access to IQVIA's proprietary offerings to certain third-party vendors, such as software vendors working for the client. SOF ¶ 188; *see also* SOF ¶¶ 188-216 (detailing provisions in IQVIA's Third Party Access agreements and the Third Party Access program). To respond to clients' requests, while still protecting its intellectual property, IQVIA created its Third Party Access program in 1991. SOF ¶¶ 188-89. Over [redacted] vendors participate in the Third Party Access program. SOF ¶ 190. IQVIA later developed the

web-based Third Party Access portal as a way for clients to submit Third Party Access requests and for IQVIA to evaluate them in a more streamlined fashion. SOF ¶ 192. As part of a Third Party Access request, IQVIA requires the client to provide information about the vendor, the IQVIA data offering(s) to be hosted, accessed, and used by the vendor, and the intended use(s) of the IQVIA data by the vendor. SOF ¶ 193.

After the vendor submits the necessary information, the product managers or "owners" of the relevant IQVIA offering evaluate the request pursuant to a defined set of procedures and criteria. SOF ¶ 196. When the third-party vendor poses a higher risk to IQVIA's intellectual property, the Third Party Access request is subject to a more thorough, manual review. SOF ¶¶ 198-200. If an IQVIA product owner, after a manual review, remains concerned about the intellectual property or other risks associated with a particular request, the request is elevated to IQVIA's in-house counsel for a final determination. SOF ¶ 201. If the request is approved following IQVIA's review, IQVIA sends a Third Party Access license agreement with IQVIA's signature to the vendor's authorized signer. SOF ¶ 202.

That Third Party Access agreement is a limited-use license agreement that contains safeguards to protect the confidentiality of IQVIA's market research offerings. SOF ¶ 204. The license is limited to specific permitted use definitions explicitly defined in the agreement. SOF ¶¶ 205-06. The vendor is required to agree not to use the licensed IQVIA data, or any information and materials derived from that data, for any purpose ***other than*** solely to benefit the mutual client. SOF ¶ 207. The vendor also agrees to refrain from disclosing the licensed IQVIA data and any derivations to anyone other than IQVIA or the client and only to its employees that need access to the data for the uses specified in the agreement. SOF ¶ 209.

Historically, IQVIA had primarily granted Third Party Access licenses to Veeva for one particular use only: to host IQVIA's data offerings in Veeva's customer relationship management ("CRM") software.[4] SOF ¶ 213. Under these Third Party Access licenses, Veeva has expressly agreed that IQVIA's data, including OneKey, DDD, and Xponent, are "proprietary to IQVIA" and that any "misuse or misappropriation of IQVIA Data and associated intellectual property" "may result in substantial and potentially irreparable injury to IQVIA's business." SOF ¶ 214. In order to obtain access to IQVIA's offerings, Veeva "acknowledged and agreed that IMS Data, and all intellectual property rights thereto, shall remain the sole and exclusive property of IMS." SOF ¶ 216. In addition, Veeva agreed that it would ***not*** use IQVIA's offerings to directly or indirectly "enhance, improve, update, validate, create, develop, [or] benchmark" Veeva's own "data, information, technology, methodology or other intellectual, proprietary, or intangible property." SOF ¶¶ 208, 251.

B. Veeva Enters the Data Business

Veeva was founded in 2007 and initially provided CRM software to the life sciences industry. SOF ¶¶ 217-20. Many pharmaceutical companies began to use Veeva's CRM software. SOF ¶ 220. But while Veeva had success in the CRM software business, it became envious of IQVIA's data business. Many of Veeva's CRM customers licensed the data maintained in Veeva's CRM from IQVIA. SOF ¶ 221. Veeva's industry experience gave it insight into how successful and valuable IQVIA's offerings were—for example, Veeva believed that the "budget" for IQVIA's

[4] CRM is a tool used by businesses—frequently their sales forces—to organize and track their interactions with customers (e.g., HCPs in the case of life sciences companies). SOF ¶¶ 218-19. Veeva describes itself as the "dominant" CRM provider in the life sciences industry. SOF ¶¶ 13, 220.

products was "clearly bigger than [Veeva's] CRM budgets. Maybe not double, but close to it." SOF ¶ 222. So Veeva decided it wanted to sell data too.

In May 2013, mere months before it became a public company in October 2013, Veeva announced a new product, Veeva Network. SOF ¶¶ 223, 229. The product was to be a combination of Master Data Management ("MDM") software[5] and a reference data product that would compete with IQVIA's OneKey offering. SOF ¶¶ 223-25. Veeva's reference data product, which it later called Veeva OpenData,[6] was Veeva's first foray into healthcare information offerings. SOF ¶¶ 228-34. When Veeva made this announcement, however, ***it did not actually have*** a reference data offering nor a plan for building one. SOF ¶ 228. Veeva also had no expertise in healthcare information offerings, and no intention of spending the substantial time and hundreds millions of dollars that IQVIA had spent to develop OneKey. SOF ¶¶ 231-34. So Veeva scrambled to find a shortcut to "[r]ip and replace" IQVIA. SOF ¶ 230; PX0454 at '240.

Veeva's solution was to buy a data company on the cheap that had a basic dataset that Veeva could use as its starter set, and then use what Veeva called "crowdsourcing" to build it out. SOF ¶¶ 235-36. Veeva's co-founder and former President, Matthew Wallach, instructed that Veeva "absolutely should not create our own database from primary sources. This has been done many, many times. We can just buy it. Cheap." SOF ¶ 237. Veeva cheaply acquired AdvantageMS, a small company in Fort Washington, Pennsylvania, in June 2013. SOF ¶¶ 238-43. While IQVIA paid over $500 million to acquire OneKey from Cegedim, SOF ¶¶ 32, 72, Veeva

---

[5] MDM software is used to clean, reconcile, and enrich data obtained from various sources into a single "master" set of data. SOF ¶ 224.

[6] Veeva originally launched its stand-alone data product under the name "OpenKey." Veeva CEO Peter Gassner "like[d] OpenKey because it is similar to OneKey," the competing IQVIA offering, and stated that he "know[s] there will be some confusion between OneKey and OpenKey." SOF ¶¶ 225-26. In response to an IQVIA lawsuit, Veeva rebranded its product as Veeva OpenData. SOF ¶ 227.

paid a mere $10.5 million to acquire AdvantageMS. SOF ¶ 238. AdvantageMS was a data services company that performed limited projects, such as data management, for some pharmaceutical companies (including several of IQVIA's clients). SOF ¶ 239. To perform some of this work, it maintained a limited dataset of reference data, which it housed in an internal database called "HDM." SOF ¶ 240. After Veeva bought AdvantageMS in June 2013, Veeva made the reference data contained within HDM the foundation for Veeva OpenData and AdvantageMS's team became Veeva's OpenData team. SOF ¶¶ 241-42.

Veeva got what it paid for—a cheap, low-quality reference data set. SOF ¶¶ 243-47. Veeva's internal quality tests revealed, for example, that the addresses for HCPs in Veeva's dataset—a key component of any HCP reference dataset—were ***less than*** [redacted] ***accurate***, well below industry standards. SOF ¶ 244. Veeva OpenData also had phone records for only "[redacted] of our records," far below the [redacted] that Veeva needed to be competitive. SOF ¶ 246. In short, Veeva knew that its starter dataset was not commercially viable. SOF ¶¶ 243-47.

Veeva's hope was that its "crowdsourcing" idea would be a quick and easy shortcut to make its offering commercially viable. Veeva's plan was to exploit the data that Veeva's customers stored in Veeva CRM—which those customers had often licensed from IQVIA—to improve Veeva's own reference data. SOF ¶¶ 248-53. Veeva publicly boasted about this "crowdsourcing" strategy: "We already have 55 million provider records in our [CRM] system," and so "we will be able to merge these records and provide the best available master data." SOF ¶ 249; PX0342. As Veeva was eventually forced to accept, though, this crowdsourcing strategy was illegal. SOF ¶ 253. The 55 million records that Veeva bragged it had in its CRM system were, to a large degree, composed of "***data that customers have licensed from IQVIA***" and other competitors like Cegedim. SOF ¶ 250. Veeva had access to this IQVIA data only pursuant

to the limited license terms of its Third Party Access agreements with IQVIA discussed above, which clearly and explicitly prohibited Veeva from using its access to IQVIA data to improve its own offerings. SOF ¶¶ 188-216 (describing terms of Third Party Access agreements). Crowdsourcing IQVIA data to build Veeva's competing offering would have amounted to blatant theft out in the open, and so Veeva was forced to scrap this "bad idea." SOF ¶¶ 252-53.

C. Veeva's Misappropriation Of IQVIA's Proprietary Offerings

Veeva did not have a Plan B. Some Veeva data employees and managers advocated for investing more money and resources into additional data sources. SOF ¶ 254. But these attempts were vetoed by Veeva's top executives, including its CEO Peter Gassner. SOF ¶ 255. Having rashly announced it was launching a reference data offering, Veeva's only remaining option for delivering on what it had promised to the marketplace before its initial public offering was to engage in misappropriation from IQVIA in secret.

1. Veeva Uses IQVIA's Proprietary Offerings to Build Veeva OpenData in HDM

As noted, Veeva knew that the AdvantageMS reference data Veeva acquired was of such low quality that it was not commercially viable. SOF ¶¶ 243-47. This was no surprise—Veeva executives described AdvantageMS as having a "mom and pop shop mentality," made up of "generally a bunch of boneheads," and a "POS company." SOF ¶ 256. Indeed, Veeva described AdvantageMS as a "house of cards," and a "f'ing waste of money." SOF ¶ 256. But AdvantageMS did have one advantage—the minor "data services" projects that it had been doing for clients for years meant that it was receiving a steady feed of millions of IQVIA's proprietary data records. SOF ¶¶ 239, 257-58. After Veeva acquired AdvantageMS, it had access to these feeds of IQVIA data too. SOF ¶¶ 259-64.

Veeva exploited this advantage in two ways, as documented in the "OpenData Data Corruption Memo." SOF ¶¶ 265-75; PX0293.

First, Veeva configured its algorithms to programmatically feed IQVIA proprietary data into Veeva OpenData. SOF ¶¶ 265-72. The OpenData Data Corruption Memo confirms that IQVIA's proprietary offerings, contained within Veeva's HDM database, were "***programmatically included within Veeva OpenData***," such that "***IMS data provided by a customer***" contributed to "***the OpenData golden data set that is distributed to customers via Network***." SOF ¶ 265; PX0293 at '832-33. Veeva knew that "***[t]his issue breaks contract agreements***" and "***contributes IMS data***" into Veeva OpenData. SOF ¶ 266; PX0293 at '833.

IQVIA expert, Michael Perry, estimates that this programmatic theft implicated over two million IQVIA data records from just one single IQVIA client—[redacted] SOF ¶ 268; PX0359 ¶ 108. But that is only the tip of the iceberg—Veeva identified nine other IQVIA customers from which it programmatically included IQVIA data into Veeva OpenData. SOF ¶¶ 270-71.[7] But as detailed below, *infra* at 24-26, Veeva engaged in a massive spoliation campaign that resulted in the permanent deletion of reams of records associated with HDM—the exact records IQVIA's experts would need to recreate the granular details of Veeva's programmatic misappropriation. SOF ¶ 272.

Second, Veeva provided its OpenData data stewards (researchers responsible for updating Veeva OpenData) full access to IQVIA's proprietary offerings. Veeva made IQVIA's proprietary offerings "***visible to all data stewards within [the] HDM application***," so these data stewards were able to rely on IQVIA's proprietary offerings "***to improve OpenData***." SOF ¶¶ 273-81. In fact,

[7] *See also* Dkt. 349 (Sanctions Order) at 70 (finding that Veeva had "programmatically included IQVIA address records as a source in Veeva's 'best address' algorithm to verify address records in OpenData").

Veeva made "***the entire set of IMS data visible to Veeva OpenData stewards***." SOF ¶ 274 (emphasis added); *see also* Dkt. 349 (Sanctions Order) at 70 ("[T]he database storing [IQVIA's] records was viewable by Veeva's OpenData data stewards, who were responsible for improving and maintaining Veeva OpenData.").

In the fall of 2015, as part of third-party access negotiations among [redacted] IQVIA, and Veeva, Veeva agreed to a formal assessment of its systems and supposed protections. SOF ¶ 376; *see also* SOF ¶¶ 376-87 (explaining how Veeva realized the [redacted] assessment would reveal its misappropriation). Realizing the auditors would uncover Veeva's rampant theft, Veeva engaged in a massive deletion campaign (described as a "cleanup" campaign), at the direction of CEO Gassner, to deceive the auditors. SOF ¶ 396; *see generally* SOF ¶¶ 376-450 (demonstrating that Veeva orchestrated a cover-up to conceal its misappropriation). Meanwhile, Veeva also lied to IQVIA and the broader marketplace, claiming it was impossible for Veeva to use IQVIA's proprietary offerings to improve Veeva OpenData. SOF ¶¶ 311, 377, 392.

Veeva has previewed in the report of its expert Bruce Hartley that it will argue that this vast misappropriation was accidental and that legacy AdvantageMS personnel were to blame. PX0367 ¶¶ 26-28, 139-44. The evidence does not support Veeva's effort to avoid responsibility for the misappropriation that occurred, by Veeva's own admission, ***after*** it acquired AdvantageMS. Veeva's then-head of Veeva OpenData, Tim Slevin, testified that Veeva was well aware of the issues relating to the misuse of IQVIA data at the time it was building Veeva OpenData, and admitted that ***Veeva*** was responsible for the data corruption that resulted from Veeva's use of HDM. SOF ¶ 259. Slevin further testified that "[i]t wasn't a mystery" which information in HDM belonged to IQVIA, because "the data sources had names and data layouts and descriptions. So you understood the data that you were working with . . . ." SOF ¶ 260. A Senior Director of Veeva

OpenData, James Kahan, similarly testified he "knew [redacted] had been sending a set of IMS data files to AMS and then to Veeva on a weekly basis for years." SOF ¶¶ 261-63.

2. Veeva Misappropriates IQVIA's Proprietary Offerings Via Its Data Report Card Program

In late 2013, Veeva launched its "Data Report Card" or "Scorecard" program, which was another method it used to improperly access and use IQVIA's proprietary offerings to improve OpenData. SOF ¶ 282; *see generally* SOF ¶¶ 282-338 (describing Veeva's misappropriation through its Data Report Card program). Veeva knew that there was "no way" IQVIA would ever let Veeva "grade" or "score" its proprietary data, as this was flatly prohibited by IQVIA's Third Party Access licenses. SOF ¶ 283. So Veeva hid this program from IQVIA and never received any authorization from IQVIA to use its data in this way. Instead, Veeva would request approval from an IQVIA data customer to access IQVIA's data, without telling IQVIA, even when Veeva ***knew*** the data was licensed from IQVIA. SOF ¶¶ 284-97. Veeva's general counsel drafted a basic form email requesting this approval from clients, claiming that this form should not have been used when Veeva personnel knew the client licensed its data from IQVIA. SOF ¶ 291. But Veeva's OpenData team used this form email for three years anyway, even for clients who they ***actually knew*** licensed data from IQVIA. SOF ¶¶ 291-96. If the customer representative wrote back with a simple "approved," Veeva proceeded to access the data the customer licensed from IQVIA—and send it to Veeva OpenData personnel. SOF ¶ 297.

Again, Veeva did all of this even though it knew that all of the Third Party Access agreements it had signed with IQVIA expressly prohibited Veeva from using IQVIA data for any benchmarking or comparison purposes. Veeva was well aware its conduct violated the license terms and breached the obligations IQVIA put in place to protect the confidentiality of its trade secrets. SOF ¶¶ 284-89

But Veeva did not stop there. Veeva used the program not just to improperly ***acquire*** IQVIA's proprietary data, but also to ***use*** IQVIA's data for the unauthorized purpose of improving Veeva OpenData. SOF ¶¶ 306-10. As Veeva's James Kahan explained, Veeva used "the results of the Data Report Cards to ***identify any potential gaps*** in the Veeva reference data and proactively have our data stewardship team do the research and ***work to fill those gaps well before a client goes live***." SOF ¶¶ 306-10. Not coincidentally, someone at Veeva destroyed Mr. Kahan's emails from the core period of his involvement in this program. SOF ¶ 307. And while Veeva told clients it would delete the stolen data after the report card process was done, Veeva often kept it on Veeva shared drives and made it accessible to Veeva's entire OpenData team. SOF ¶¶ 308-09. As one Veeva employee stated in reporting Veeva's "Data Report Card Reuse" to a Veeva executive in a July 2014 email, "[m]y concerns are . . . [w]e may be re-using the customer data for a purpose other than a DRC . . . doing this should be impossible, if we had truly destroyed the data." SOF ¶ 309. At the same time, Veeva was falsely swearing to IQVIA that none of its employees working on Veeva OpenData could possibly ever access IQVIA's proprietary data. SOF ¶¶ 310-11.

In running Data Report Cards on IQVIA's proprietary data offerings ***at least*** [redacted] ***times***, Veeva gained access to a substantial portion of those offerings. SOF ¶¶ 312-14. Veeva was able to identify and fill gaps in Veeva OpenData and thus improve the quality of its own data. SOF ¶¶ 306-10. For example, under the pretense of a Data Report Card for IQVIA's client [redacted], Veeva extracted IQVIA's proprietary data that [redacted] had hosted in Veeva CRM, despite knowing that [redacted] subscribed to OneKey. SOF ¶¶ 316-18. The data records Veeva extracted for this "report card" themselves included IQVIA's reference codes. SOF ¶ 319. And while Veeva has since destroyed the underlying extract (so IQVIA cannot now identify every individual record that Veeva illicitly used), it did not destroy evidence showing

that this single "report card" alone involved Veeva improperly acquiring over ***2 million IQVIA records*** (approximately 1.67 million HCPs and 485,000 HCOs). SOF ¶¶ 320-22. If each of the 44 or more report card analyses were of a similar scale, Veeva misappropriated roughly ***100 million*** IQVIA records through its report card program (potentially billions of IQVIA data values, as each record contains dozens of fields).

IQVIA learned about this illegal misappropriation campaign only due to the actions of a conscientious client, [redacted] SOF ¶¶ 324-38. Veeva accessed and extracted mutual client [redacted]'s data from its CRM environment twice, in 2015 and 2016, after securing "approval" from low-level [redacted] employees who had no reason to be aware of the license restrictions imposed by IQVIA. SOF ¶¶ 324, 328-33. But Veeva knew that [redacted] licensed OneKey from IQVIA. SOF ¶ 325. When [redacted] leadership found out about Veeva's improper extraction of IQVIA's proprietary data, it considered it to be a data breach by Veeva and notified IQVIA. SOF ¶¶ 326-27. Veeva executives internally admitted that Veeva's actions involving the [redacted] Data Report Cards were "filled with bad choices" by Veeva. SOF ¶¶ 335-36. The [redacted] data breach was one of several facts IQVIA considered in deciding to file this lawsuit. SOF ¶ 338.

3. Veeva Misappropriates IQVIA's Proprietary Offerings Via "Early Adopters"

As yet another avenue of theft, Veeva targeted a few "early adopters" to whom it offered OpenData at rock-bottom prices that pressured them to switch away from IQVIA's data. SOF ¶¶ 339-63. Veeva then pressured these companies to send them IQVIA's proprietary data and other sensitive internal documents, which Veeva used to further improve Veeva OpenData. SOF ¶¶ 339-63.

[redacted] is an example. Veeva represented to [redacted] that it could provide IQVIA OneKey-level quality at a bargain price. SOF ¶¶ 340-44. As explained by [redacted], the person

in charge at [redacted] during the switch, [redacted] selected Veeva "OpenData because the price was lower assuming that it was the same quality" as IQVIA's data, but that turned out to be "not true." SOF ¶¶ 344-45. After [redacted] switched to Veeva OpenData, it immediately complained to Veeva that there were "major major gap[s]" in Veeva's data. SOF ¶¶ 346-53. To fill those gaps, Veeva pressured [redacted] personnel to send reams of IQVIA proprietary information to Veeva. SOF ¶¶ 354-56.

As just one example of Veeva's misappropriation during this project, on December 29, 2015, Veeva improperly obtained from [redacted] an "updated file with hospitals, parents and outlets," which was a spreadsheet of 11,531 OneKey records belonging to IQVIA. SOF ¶¶ 357-59. Veeva has admitted it did not receive a Third Party Access license agreement that would allow its receipt or use of these records. SOF ¶ 359. This information contained valuable and proprietary affiliation information between and among IQVIA records, showing how various HCOs (called outlets) map to larger hospitals and hospital systems. SOF ¶¶ 358-63. This is one of the few files that Veeva did not destroy as part of its spoliation campaign, and thus IQVIA can demonstrate what these files looked like and identify every record in them.

Through [redacted], Veeva also improperly obtained and analyzed proprietary documentation about how IQVIA structures its Healthcare Professional and Organizational Data products in terms of field names, classifications, hierarchy, and organization. SOF ¶ 363. Veeva's theft continued in various forms with other "early adopter" customers, including [redacted] likely through the present day. SOF ¶¶ 364-75. As with HDM and Data Report Card misappropriation, the full extent of Veeva's misappropriation through OpenData early adopters can never be known due to Veeva's extensive spoliation. SOF ¶¶ 371-73.

D. Veeva Orchestrates A Cover-Up To Conceal Its Misappropriation

Veeva engaged in a purposeful, widescale deletion of records designed to make it impossible for IQVIA to identify the full scope and scale of Veeva's misappropriation in a lawsuit. SOF ¶¶ 376-450.

In connection with the audit in the fall of 2015, Veeva recognized that if the audit proceeded as planned, it would expose that Veeva had been improperly using IQVIA's proprietary offerings, without permission or authorization, to build Veeva OpenData for years. SOF ¶¶ 376-87. Veeva executives prepared a document they called the "OpenData Data Corruption Memo" for Veeva CEO Gassner detailing, among other things, Veeva's programmatic inclusion of IQVIA's proprietary offerings in Veeva OpenData via HDM as well as Veeva OpenData data stewards' unauthorized access to IQVIA's proprietary offerings. SOF ¶ 383; PX0293. As set forth in the OpenData Data Corruption Memo, Veeva's management explained to Gassner that "the Audit has a high likelihood of exposing" Veeva's improper use of IQVIA's proprietary offerings, and recommended that Veeva "Delay Audit" as a result. SOF ¶ 383; PX0293 at '826.

Veeva did, in fact, delay the audit twice, falsely claiming it needed more time to deal with the paperwork. SOF ¶ 387. While this was happening, Veeva's management discussed how to respond to the reality that IQVIA "***will file a lawsuit against Veeva for damages***" as a result of Veeva's misappropriation. SOF ¶ 385; PX0293 at '831. As Judge Cavanaugh found, the "OpenData Corruption Memo indicates that Veeva was well-aware that it was misappropriating IQVIA data, something the [redacted] Audit would uncover, and that the incident could lead to litigation." Dkt. 349 (Sanctions Order) at 75. Veeva management presented the OpenData Data Corruption Memo to CEO Gassner on September 29, 2015, and recommended that Veeva disclose its misuse of IQVIA's proprietary offerings to IQVIA, customers, and the general public. SOF ¶¶ 388-90.

But Gassner overruled this plan, instead deciding Veeva would not tell IQVIA or anyone else what Veeva had done and would instead cover it up. SOF ¶ 391. Gassner wrote to [redacted] IQVIA's [redacted] falsely representing that "there is no suggestion that IMS OneKey data has been mishandled by Veeva" and that Veeva's systems "protect IMS IP." SOF ¶ 392. At Gassner's direction, Veeva then began systematically deleting the evidence of its misappropriation. SOF ¶¶ 396-450. The fabrications that Veeva advanced in September 2015 are the same ones Veeva is telling the Court now.

As Judge Cavanaugh found, Veeva "engaged in an extensive clean-up endeavor to hide what had occurred" and "actively and purposefully deleted evidence" related to HDM, "knowing that [an] audit would likely uncover" its misappropriation of IQVIA's proprietary offerings. Dkt. 349 (Sanctions Order) at 72. Among other things, Veeva deleted over 200 file directories and thousands of tables within its HDM database—each of which would have shown the specific ways that Veeva misused IQVIA's proprietary offerings to build Veeva OpenData. SOF ¶¶ 397-412; Dkt. 583 (Mar. 30, 2024 Order) at 8. A single IQVIA data file deleted from one of the 200 directories could contain several millions of IQVIA data records (as was the case for the [redacted] extract). The volume of IQVIA information deleted can never be known, but it could very well range into the hundreds of millions of records (and thus potentially billions of IQVIA data values, as each record contains many data fields). As for the HDM tables, while the underlying records are gone, the names of the tables deleted by Veeva often give away what Veeva tried to hide—that they contained IQVIA's market research offerings. SOF ¶¶ 402-12.

Veeva also destroyed substantial evidence relating to its Data Report Card program, both before and after this case was filed. Veeva deleted 17-months' worth of emails involving [redacted] from the very time period in which he was involved in running the program. SOF

¶¶ 420-22; Dkt. 349 (Sanctions Order) at 86-88. Moreover, ***after*** IQVIA filed its complaint against Veeva in this case, Veeva created the Data Destroyed Spreadsheet, which provides a record of Veeva's efforts to identify and destroy incriminating evidence in the months after IQVIA filed this lawsuit. SOF ¶¶ 423-32; PX0309. The Data Destroyed Spreadsheet shows that, even just considering the period after this lawsuit was filed, Veeva destroyed the IQVIA data it used to run at least 21 Data Report Cards. SOF ¶¶ 423-32; PX0309.

LEGAL STANDARD

"A party may move for summary judgment, identifying each claim or defense—or the part of each claim or defense—on which summary judgment is sought." Fed. R. Civ. P. 56(a). "The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." *Id.*

"By its very terms, this standard provides that the mere existence of *some* alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247–48 (1986). "Only disputes over facts that might affect the outcome of the suit" can "preclude the entry of summary judgment." *Id.* at 248. "When the moving party has carried its burden under Rule 56(c), its opponent must do more than simply show that there is some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). "If the evidence [offered by the non-moving party] is merely colorable, or is not significantly probative, summary judgment may be granted." *Anderson*, 477 U.S. at 249–50 (citations omitted).

IQVIA has brought trade secret claims under both the Defend Trade Secrets Act ("DTSA")[8] and applicable state law, the New Jersey Trade Secrets Act ("NJTSA").[9] Both statutes contain "virtually identical definitions of trade secret, misappropriation, and improper means," and, as a result, "the analysis under DTSA folds into that of NJTSA." *Austar Int'l Ltd. v. AustarPharma LLC*, 425 F. Supp. 3d 336, 355 (D.N.J. 2019); *see also Oakwood Lab'ys LLC v. Thanoo*, 999 F.3d 892, 905 n.11 (3d Cir. 2021) (DTSA and NJTSA are "substantially similar"); *Corp. Synergies Grp. v. Andrews*, 2019 WL 3780098, at *3 (D.N.J. Aug. 12, 2019). "Both the DTSA and the NJTSA require claimants to demonstrate (1) the existence of a trade secret, defined broadly as information with independent economic value that the owner has taken reasonable measures to keep secret, and (2) misappropriation of that secret[.]" *Par Pharm., Inc. v. QuVa Pharma, Inc.*, 764 F. App'x 273, 278 (3d Cir. 2019). "There are three ways to establish misappropriation under the DTSA: improper acquisition, disclosure, or use of a trade secret without consent." *Oakwood*, 999 F.3d at 907–08.

[8] For IQVIA's federal law claim (Count I), the DTSA applies because Veeva continued its misappropriation of IQVIA's trade secrets after May 11, 2016, the date of the DTSA's enactment. *See Nasdaq Inc. v. Miami Int'l Holdings, Inc.*, 2023 WL 4740753, at *4 (D.N.J. July 25, 2023). The DTSA also requires that the asserted trade secret be "related to a product or service used in, or intended for use in, interstate or foreign commerce," 18 U.S.C. § 1836(b)(1), and OneKey, DDD, and Xponent are each used nationally and/or internationally. SOF ¶¶ 5, 17-18, 23.

[9] The NJTSA applies to IQVIA's state-law claim (Count II). Under New Jersey choice-of-law principles, which govern state law claims in this District, "the place of alleged misappropriation is controlling." Dkt. 90 at 8. Much of Veeva's misappropriation occurred in Fort Washington, Pennsylvania, where Veeva's OpenData team was based. SOF ¶¶ 256-363. Because Pennsylvania and New Jersey trade secret laws are "identical," *Elmagin Cap., LLC v. Chen*, 2022 WL 1172970, at *3 (E.D. Pa. Apr. 20, 2022), "there is no actual conflict," and "the court applies the law of the forum state." *Arcand v. Brother Int'l Corp.*, 673 F. Supp. 2d 282, 293 (D.N.J. 2009).

ARGUMENT

I. IQVIA'S PROPRIETARY OFFERINGS QUALIFY FOR TRADE SECRET PROTECTION

IQVIA's OneKey, DDD, and Xponent offerings indisputably qualify for trade secret protection as confidential compilations of market research information under federal and state law. The DTSA broadly defines a trade secret as "all forms and types of financial, business, scientific, technical, economic, or engineering information," including "***compilations***," if "the owner thereof has taken reasonable measures to keep such information secret," and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by[] another . . ." 18 U.S.C. § 1839(3) (emphasis added); *see also* N.J. Stat. Ann. § 56:15-2 (defining a trade secret along similar parameters and expressly including a "business data ***compilation***" (emphasis added)).

A. IQVIA Has Sufficiently Identified Its Proprietary Compilations As Its Asserted Trade Secrets

IQVIA has identified its OneKey, Xponent, and DDD market research offerings as the trade secrets Veeva misappropriated. "A trade secret is defined with particularity when the trade secret can be distinctly separated from 'matters of general knowledge in the trade or [from] special knowledge of those persons who are skilled in the trade.'" *Talon Indus., LLC v. Rolled Metal Prod., Inc.*, 2022 WL 3754800, at *10 (D.N.J. Aug. 30, 2022) (alteration in original) (quoting *Oakwood*, 999 F.3d at 906). Where "a plaintiff provides a general description and offers specific examples of protectable elements of the general design, courts have found a plaintiff has adequately defined a trade secret." *Id.*; *see also Absorption Pharms., LLC v. Reckitt Benckiser LLC*, 2020 WL 10139487, at *10 (D.N.J. June 25, 2020) (holding at summary judgment that plaintiff had sufficiently identified trade secrets, including "online cart information, consumer insight and behavior," and "sales data and trends").

IQVIA's proprietary offerings constitute valuable compilations of healthcare information built from IQVIA's market research, data acquisition and analysis, and sophisticated algorithms and processes. SOF ¶¶ 68-101 (IQVIA's investments to create and maintain OneKey); SOF ¶¶ 102-38 (IQVIA's investments to create and maintain DDD and Xponent); SOF ¶¶ 139-42 (IQVIA's revenue from licensing OneKey, DDD, and Xponent). Such compilations are "classic examples of a trade secret that derives from an amalgam of public and propriety source data" that "cumulatively" were the "product of years of effort and expense." *United States v. Nosal*, 844 F.3d 1024, 1042 (9th Cir. 2016).[10] At this Court's direction, IQVIA provided a comprehensive, 112-page discovery response laying out the basis for this identification in great detail. SOF ¶ 26. That response extensively describes IQVIA's proprietary offerings, including by providing exemplar records and fields, details about how they are built, and screenshots of the proprietary offerings themselves. SOF ¶ 26. IQVIA's response also describes Veeva's misappropriation of IQVIA's proprietary offerings, including by identifying dozens of specific exports of IQVIA's offerings that Veeva misappropriated. SOF ¶ 26.

Magistrate Judge Allen held that IQVIA's interrogatory response sufficiently identified and described IQVIA's proprietary offerings with particularity, including because IQVIA's response contains significant discussion about the type of information IQVIA's offerings provide, "explain[s] in detail" the "host of proprietary processes" IQVIA uses to build its offerings, and lays out Veeva's alleged misappropriation and "specifically references information in the way of

[10] *Accord Allstate Life Ins. Co. v. Stillwell*, 2019 WL 2743697, at *10 (D.N.J. May 16, 2019) (granting summary judgment on trade secret misappropriation and holding that "Plaintiff's collection of client names, addresses, and telephone numbers constituted a trade secret because it can be described as a 'business data compilation'"); *Synthes, Inc. v. Emerge Med., Inc.*, 25 F. Supp. 3d 617, 706 (E.D. Pa. 2014) (granting summary judgment on trade secret misappropriation, because "[a] compilation of data that has independent economic value can be protected as a trade secret" (citations omitted)).

spreadsheets [that were allegedly misappropriated]." Dkt. 539-5 (June 1, 2023 Hearing Tr.) 82:8-85:13.[11] This Court, in turn, held that "Magistrate Judge Allen correctly found that IQVIA identified the alleged trade secrets with 'reasonable particularly in its responses to' Veeva's Interrogatories." Dkt. 581 at 8 (citation omitted).

Veeva has tried to mislead the Court by arguing that IQVIA has failed to identify all of the individual pieces of data that Veeva misappropriated from the compilations. But IQVIA is not seeking "statutory trade secret protection for individual pieces of information"; rather, IQVIA "seek[s] protection over the ***compilations*** of this information . . . that [IQVIA] has created and developed over years . . . ." *IHS Glob. Ltd. v. Trade Data Monitor, LLC*, 2021 WL 2134909, at *7 (D.S.C. May 21, 2021) (emphasis added). Accordingly, the proper inquiry for trade secret identification is whether IQVIA's proprietary offerings, as compilations, meet the statutory elements for trade secret protection ***as a whole***. Thus, as other courts have recognized, Veeva's request that the Court "isolate certain pieces of information and rule that each, individually, is not entitled to trade secret protection," should be rejected, since IQVIA "seek[s] protection under the relevant statutes for compiled lists and databases, not the individual pieces of information contained therein." *Id.*; *see also Uhlig LLC v. Shirley*, 2012 WL 2923242, at *6 (D.S.C. July 17, 2012) (rejecting defendant's argument that "identification of the compilation trade secrets at trial" required plaintiff to identify "each and every document" underlying the compilation because it was devoid of "any authority"); *DiscoverOrg Data, LLC v. ThisWay Glob., LLC*, 2020 WL 10054509,

[11] IQVIA has since provided Veeva with further detail regarding IQVIA's proprietary offerings (and how Veeva misused them), including in the reports of four separate experts. [redacted] (describing IQVIA's proprietary offerings and how they generate value via their secrecy); [redacted] (describing how IQVIA protects the secrecy of its offerings); [redacted] (detailing Veeva's misappropriation).

at *2 (W.D. Tex. Dec. 1, 2020) (rejecting argument that plaintiff must identify as a trade secret the specific "subset of information" from a larger database of information that was misused).

Moreover, despite its tactical claims of ignorance in this litigation, Veeva is very familiar with IQVIA's proprietary offerings. In numerous agreements with IQVIA, Veeva has agreed to protect the confidentiality of these exact proprietary offerings ***by name***. SOF ¶ 214. Veeva's experts have also testified that they understand IQVIA's proprietary offerings. SOF ¶ 29; *see Rohm & Haas Co. v. Adco Chem. Co.*, 689 F.2d 424, 432 n.7 (3d Cir. 1982) (reversing the district court's holding that plaintiff had "failed to adequately define its alleged trade secret" where defendant's expert "testified that he understood plaintiff's statement of its claimed trade secret").

IQVIA has, therefore, sufficiently identified its proprietary offerings as its trade secrets under black-letter law.

B. IQVIA's Proprietary Offerings Are Protectable

IQVIA's identified offerings qualify for trade secret protection because IQVIA derives substantial economic value from each of them as a result of the reasonable measures it has taken to ensure they are secret and not readily ascertainable. *See* 18 U.S.C. § 1839(3); N.J. Stat. Ann. § 56:15-2.

IQVIA indisputably derives actual economic value from its OneKey, DDD, and Xponent offerings. IQVIA earns [redacted] in revenue each year by licensing its OneKey, DDD, and Xponent offerings to clients. SOF ¶¶ 139-42; *see Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1291 (11th Cir. 2003) (affirming district court's finding of trade secret status because "it is clear that [plaintiff's] information possessed actual or potential economic value; after all, [defendants] were negotiating with [plaintiff] for a potential licensing agreement at the time of the purported misappropriation"); *Events Media Network, Inc. v. Weather Channel Interactive, Inc.*, 2013 WL 3658823, at *3 (D.N.J. July 12, 2013) (finding that licensing agreements for access

to compilation "indicate that the party values the information in compilation form and is willing to pay the owner for its use").[12] IQVIA's clients pay for these licenses because of the value they receive from using IQVIA's proprietary offerings in their sales, marketing, and research efforts (among other things). SOF ¶¶ 45-67.

It is equally clear that IQVIA derives this economic value from its offerings because it has taken reasonable steps to keep them secret, thus ensuring they are not available in or reasonably ascertainable from the public domain. IQVIA has gone to great lengths to protect the secrecy of its proprietary offerings, including via physical and IT security measures,[13] employee confidentiality training and non-disclosure agreements, and robust license and Third Party Access agreements with outside parties. SOF ¶¶ 143-216. These measures easily meet—in fact, exceed—the "reasonable measures" required by trade secret law. *See, e.g.*, *United States v. Xue*, 2023 WL 4622816, at *1 (3d Cir. July 19, 2023) (courts have found a "company's physical and digital security, nondisclosure agreements, and training on confidentiality" are "reasonable to maintain secrecy"); *Syncsort Inc. v. Innovative Routines, Int'l, Inc.*, 2011 WL 3651331, at *15 (D.N.J. Aug. 18, 2011) (granting summary judgment on trade secret misappropriation where plaintiff required outside parties to sign license agreements); *Synthes, Inc. v. Emerge Med., Inc.*, 25 F. Supp. 3d 617, 707 (E.D. Pa. 2014) (granting summary judgment on trade secret misappropriation where plaintiff "had in place numerous measures to maintain the secrecy of this

[12] *See also Tan-Line Sun Studios, Inc. v. Bradley*, 1986 WL 3764, at *7 (E.D. Pa. Mar. 25, 1986), *aff'd*, 808 F.2d 1518 (3d Cir. 1986) ("Perhaps the best evidence supporting my holding that Tan-Line's entire methodology constitutes a trade secret is the fact that franchisees are willing to purchase the rights to use and learn the methodology.").

[13] ***Veeva's own security expert*** recognized that IQVIA's internal security satisfied the very standard he used in his own reports. SOF ¶ 167; PX0353 ¶ 39.

information, including policies, nondisclosure contracts with employees and vendors, and physical security measures").[14]

Moreover, these measures have worked. IQVIA's clients have paid [redacted] of dollars to access IQVIA's offerings because those clients cannot readily access or create these offerings in the public domain. Thus, IQVIA indisputably meets the modest burden of establishing that its offerings ***as a whole*** are not readily ascertainable. *See, e.g.*, *AvidAir Helicopter*, 663 F.3d at 973 ("The fact that information can be ultimately discerned by others—whether through independent investigation, accidental discovery, or reverse engineering—does not make it unprotectable. Instead, the court must look at whether the duplication of the information would require a substantial investment of time, effort, and energy." (citation omitted)); *Uhlig*, WL 2923242, at *7 ("Although Defendants contend that the individual components of the trade secrets could have been obtained by proper means from the customers, Defendants ignore that the value of the trade secrets is not in their individual components, but in their collective effect. Therefore, the more appropriate inquiry is whether the trade secret as a whole was readily ascertainable. [Plaintiff] presented evidence that the trade secret could not be ascertained without substantial effort.").

Veeva has suggested that IQVIA's offerings are not protectible trade secrets because ***some individual elements*** of the data within IQVIA's trade secret compilations are publicly available or made publicly available by regulation. *E.g.*, Dkt. 539-1 at 3-4, 10-12. This is a red herring. The question is not whether IQVIA's trade secret offerings include publicly available information, but

[14] *See also Allstate Life Ins. Co. v. Stillwell*, 2019 WL 2743697, at *10 (D.N.J. May 16, 2019) (trade secret law "requires only reasonable measures to be taken to protect trade secrets"); *AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F.3d 966, 974 (8th Cir. 2011) ("Reasonable efforts to maintain secrecy need not be overly extravagant, and absolute secrecy is not required.").

rather, whether IQVIA's OneKey, DDD, and Xponent offerings are publicly available as ***compilations***. *See Nosal*, 844 F.3d at 1042 ("It is well recognized that it is the secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation, or integration of the individual elements . . . ." (citation omitted)).

This is black-letter law. If it were otherwise, and "defendants were permitted to isolate pieces of information in a compiled list and ask a court to determine that each, individually, is not entitled to protection, they could eliminate trade secret protection with respect to an entire list, one item at a time," and thereby "nullify a compilation's trade secret protection by arguing that each component part is publicly available and thus not subject to protection." *IHS Glob.*, 2021 WL 2134909, at *8. "The law does not leave room for such a result." *Id.*

In fact, it is also black-letter law that a compilation may be a protectable trade secret, even if the ***entirety*** of the information therein is publicly available—which is not the case here—so long as the compilation itself is not publicly available. *See, e.g.*, *Xue*, 2023 WL 4622816, at *1 ("Even a nonpublic combination of public information can be a trade secret."); *Par Pharm.*, 764 F. App'x at 279 ("[T]hough 'each and every element of plaintiff's [asserted trade secret] may be known to the industry, the combination of those elements may be a trade secret if it produces a product superior to that of competitors'" (citation omitted)); *AirFacts, Inc. v. de Amezaga*, 909 F.3d 84, 96 (4th Cir. 2018) ("Courts have long recognized that 'a trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain'" if the

compilation "affords a competitive advantage" (citation omitted)).[15] It is beyond genuine dispute that IQVIA's offerings, when each is properly viewed ***as a whole***, are not publicly available.

C. Veeva Has Agreed That IQVIA's Proprietary Offerings Are Intellectual Property In Binding Legal Documents

This Court should also prevent Veeva from challenging the existence of IQVIA's trade secrets because Veeva has repeatedly agreed to treat these offerings as IQVIA's protectible intellectual property in binding legal documents. *See, e.g.*, *In re Uniservices, Inc.*, 517 F.2d 492, 496 (7th Cir. 1975) (party "was estopped by his prior conduct to deny that the trade routes and client service contracts are trade secrets" due to party's signing of prior agreements that assigned value to the trade secrets); *Kodekey Elecs., Inc. v. Mechanex Corp.*, 486 F.2d 449, 455 (10th Cir. 1973) (Defendant's "express agreement 'not to disclose [the trade secrets]' is a positive acknowledgement of the fact that [they] are secret; the stipulation would otherwise be meaningless" (citation omitted)).

In the dozens of Third Party Access agreements Veeva has entered into with IQVIA, Veeva ***agreed*** that IQVIA's offerings are "proprietary to IQVIA" and that "misuse or misappropriation of IQVIA Data and associated intellectual property is difficult to detect" and "may result in substantial and potentially irreparable injury to IQVIA's business." SOF ¶¶ 214-15. After ***agreeing*** that IQVIA's offerings are protectable intellectual property, Veeva should be estopped from now claiming that IQVIA's offerings are not protectable. *See Beer Nuts, Inc. v. King Nut Co.*, 477 F.2d 326, 328 (6th Cir. 1973) (holding that a trademark licensee could not challenge

---

[15] *See also Penalty Kick Mgmt.*, 318 F.3d at 1291 (same); *Radiant Glob. Logistics, Inc. v. Furstenau*, 368 F. Supp. 3d 1112, 1127 (E.D. Mich. 2019) (same); Restatement (Third) of Unfair Competition § 39 cmt. f ("The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation, or integration of the individual elements.").

validity of trademark because a "contracting party may not repudiate his promises solely because he later becomes dissatisfied with his bargain"); *Creative Gifts, Inc. v. UFO*, 235 F.3d 540, 548 (10th Cir. 2000) (same).[16]

Applying basic principles of contract law, courts recognize that a party "should not be permitted to enjoy the benefits afforded by the license agreement while simultaneously urging" that the intellectual property "which forms the basis of the agreement is void." *John C. Flood of Virginia, Inc. v. John C. Flood, Inc.*, 642 F.3d 1105, 1111 (D.C. Cir. 2011); McCarthy on Trademarks and Unfair Competition § 18:63 ("[A] licensee of intellectual property should not be permitted to enjoy the use of the licensed property while at the same time challenging that intellectual property as being invalid."); *see also First Am. Title Ins. Co. v. Leonardo*, 2008 WL 149967, at *4 (N.J. Super. Ct. App. Div. Jan. 17, 2008) ("[W]here a party affixes his signature to a written instrument, . . . a conclusive presumption arises that he read, understood and assented to its terms . . . ."). These principles bar Veeva's challenges here—especially because the agreements were executed by Veeva's General Counsel, Josh Faddis, who clearly understood these terms.

Accordingly, for all of these reasons, this Court should rule that IQVIA's market research offerings (OneKey, DDD, Xponent) are subject to protection as IQVIA's trade secrets.

---

[16] *Accord Friedman v. Quest Int'l Fragrances Co.*, 58 F. App'x 359, 360 (9th Cir. 2003) (defendant's "acknowledgment in the non-disclosure agreement" of the confidentiality of asserted trade secrets should "have some bearing" as to the determination of their protectability); *Gold Messenger, Inc. v. McGuay*, 937 P.2d 907, 911 (Colo. App. 1997) (defendant estopped from challenging protectability of trade secret because "the terms of the agreement declare that the confidential information constitutes the 'trade secrets' of [plaintiff]"); *Synthes,* 25 F. Supp. 3d at 707 (no genuine issue of material fact as to the protectability of data compilations because defendants "signed agreements recognizing" them to be "confidential information").

II. VEEVA MISAPPROPRIATED IQVIA'S PROPRIETARY OFFERINGS

The Court should also rule that Veeva has misappropriated IQVIA's proprietary offerings by acquiring them through improper means and using them without consent. "There are three ways to establish misappropriation under the DTSA: improper acquisition, disclosure, or use of a trade secret without consent." *Oakwood*, 999 F.3d at 907–08; *see also* 18 U.S.C. § 1839(5); N.J. Stat. Ann. § 56:15-2.

The DTSA defines acquisition via "improper means" to include, among other things, acquisition by "breach or inducement of a breach of a duty to maintain secrecy." 18 U.S.C. § 1839(6). Meanwhile, the "term 'use' has been broadly defined as 'any exploitation of the trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant.'" *Oakwood*, 999 F.3d at 909 (citation omitted). Use is not limited to "the narrow context of replication or obvious incorporation of trade secret-protected material in a competitor's product," as this would "exclude[] a broad range of activity that is rightly seen as unauthorized use of a trade secret and, therefore, misappropriation." *Id.* at 910. "Use" takes on an "expansive interpretation" to give "trade secret owners a fair opportunity to prove misappropriation." *Id.*; *see also id.* at 909 (listing examples that "constitute 'use'"); *Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1313 (11th Cir. 2020) (the "bar for what counts as 'use' of a trade secret is generally low").

Veeva indisputably "acquired" and "used" IQVIA's offerings without IQVIA's consent when it engaged in each of its three primary categories of misconduct discussed above. *See supra* at 17-23; SOF ¶¶ 256-363.

1. Programmatic Theft from Data Feeds. With respect to Veeva's HDM database, the Veeva data stewards responsible for building OpenData improperly acquired IQVIA's proprietary offerings when they received unfettered access to the "entire set" of IQVIA data stored in HDM.

Supra at 17-19; SOF ¶ 275. Sometimes, Veeva just acquired the data without any agreement at all, but even where Veeva had a Third Party Access agreement to use the information for some ***limited*** purpose, Veeva had express contractual duties to maintain the confidentiality of IQVIA's offerings, which specifically required Veeva to restrict Veeva's data team from any access to IQVIA's offerings. *Supra* at 13-14; SOF ¶ 209; *see also Allstate Life Ins. Co. v. Stillwell*, 2019 WL 2743697, at *11 (D.N.J. May 16, 2019) (defendants were "liable for misappropriation of trade secrets" because they "breached their explicit duties" under confidentiality agreements).

Veeva also indisputably "used" IQVIA's offerings without authorization by "employing the trade secret[s] in manufacturing or production," *Oakwood*, 999 F.3d at 909, when it incorporated IQVIA's proprietary offerings available in Veeva's HDM database and "programmatically" fed this data into its own database, *supra* at 18; SOF ¶¶ 256-81. Nor is there any dispute that Veeva lacked IQVIA's consent for this use. IQVIA's Third Party Access agreements with Veeva specifically prohibited Veeva from using IQVIA's proprietary offerings to improve Veeva's own competing data product or in any other manner that was not solely for IQVIA's client's benefit. *Supra* at 13-14; SOF ¶¶ 208, 251.

2. Grading or Scoring IQVIA's Data. Veeva likewise improperly acquired and used IQVIA's offerings without IQVIA's consent as part of its Data Report Card program. As discussed above, Veeva conducted at least [redacted] separate Data Report Cards involving IQVIA data. *Supra* at 20-22; SOF ¶¶ 282-338. Each of those "scorecards" was unauthorized even if one were to credit Veeva's paper-thin excuse that it was merely "grading" IQVIA data. Veeva's Third Party Access agreements with IQVIA prevented Veeva from using IQVIA's offerings to "benchmark" against its own competing offering. SOF ¶¶ 208, 251. *See Oakwood*, 999 F.3d at 909 ("[S]oliciting

customers through the use of information that is a trade secret" constitutes "use"). Veeva knew IQVIA would never agree to this use of its data.

Moreover, the evidence shows that Veeva did more than merely grade IQVIA's data with Veeva's Data Report Cards. Veeva's OpenData team used this access to IQVIA's data to "***fill gaps***" and improve Veeva OpenData. *Supra* at 21; SOF ¶¶ 306-10; *Oakwood*, 999 F.3d at 909 ("relying on the trade secret to assist or accelerate research or development" constitutes use). As Veeva executives admitted in internal documents, "***none of this activity was licensed or authorized*** by IMS Health with a Third-Party Access (TPA) agreement or any other document." SOF ¶ 334. Veeva's destruction of evidence relating to its use of IQVIA's offerings further shows it knew it was acting improperly. Judge Cavanaugh found that Veeva engaged in extensive spoliation precisely because it was "***well-aware*** that it was misappropriating IQVIA data" and feared the consequences of getting caught. Dkt. 349 at 7 (emphasis added); *see also Par Pharm.*, 764 F. App'x at 278 (defendant's deletion of electronic version of plaintiff's trade secret despite litigation hold "provides a basis to infer that this [defendant] employee understood he wrongly possessed and used information [plaintiff] would deem confidential").[17]

3. Soliciting IQVIA Data from Early Adopters. Finally, Veeva's improper acquisition and use of IQVIA data possessed by former IQVIA clients that were "early adopters" of Veeva OpenData represents another clear instance of misappropriation. As discussed above, Veeva solicited [redacted] among other early Veeva OpenData clients, to improperly send IQVIA data and other proprietary materials to Veeva in order to address gaps in Veeva's data that the clients

[17] *Harlan Lab'ys, Inc. v. Campbell*, 900 F. Supp. 2d 99, 109 (D. Mass. 2012) (defendant's "discard[ing] the flash drive with the confidential information" despite preservation order was "worrisome" and suggested misuse of plaintiff's "confidential information"); *Liebert Corp. v. Mazur*, 357 Ill. App. 3d 265, 282 (2005) ("The fact that Mazur attempted to destroy any indication of his downloading activities when plaintiffs filed suit also suggests improper acquisition.").

had identified. *Supra* at 22-23; SOF ¶¶ 339-75. This improper acquisition—let alone Veeva's subsequent unauthorized use of it to improve OpenData—is sufficient to give rise to liability. *See Synthes*, 25 F. Supp. 3d 617, 713 (E.D. Pa. 2014) (defendant's improper induction of third party to provide asserted trade secret in breach of confidentiality agreements "foreclose[s] any dispute of material fact as to whether he misappropriated it" and does not "require[] a showing of use").[18]

To be clear, there is substantial evidence of other acts of misappropriation by Veeva beyond those addressed in this motion. SOF ¶¶ 364-75. IQVIA is, indeed, concerned that Veeva is continuing to engage in the improper use of IQVIA's offerings and will, accordingly, seek an injunction at trial, in addition to damages. But IQVIA's motion focuses on three clear-cut examples of misappropriation beginning from Veeva's earliest efforts in 2013. There is more than sufficient evidence for the Court to rule at this stage that Veeva misappropriated IQVIA's trade secrets, based on these examples. Trial can then proceed on the scope of Veeva's misappropriation and the resulting damages.

CONCLUSION

For the reasons set forth herein, IQVIA requests that this Court hold: (1) that IQVIA's proprietary compilations of healthcare information (OneKey, DDD, and Xponent) qualify for trade secret protection under federal and state law and (2) that Veeva misappropriated those compilations by, among other things, improperly acquiring and using them to build its own competing offering, Veeva OpenData.

---

[18] Veeva cannot seriously dispute that it was well aware of the confidentiality obligations applicable to IQVIA's data clients. Veeva's license agreements for its own competing data offering contain confidentiality obligations. SOF ¶ 186. *See Syncsort Inc. v. Innovative Routines, Int'l, Inc.*, 2011 WL 3651331, at *17 (D.N.J. Aug. 18, 2011) (defendant knew its use was improper because it was "standard industry practice to market software through licensing agreements that impose confidentiality obligations on customers" and defendant was a "participant in the software development market").

Dated: June 17, 2024

/s/ Amy Luria
CRITCHLEY, KINUM & LURIA, LLC

Michael Critchley
Amy Luria
75 Livingston Avenue
Roseland, New Jersey 07068
Tel. (973) 422-9200
mcritchley@critchleylaw.com
aluria@critchleylaw.com

-and-

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Steig D. Olson
Patrick D. Curran
David S. Mader
David LeRay
Matthew Fox
51 Madison Avenue, 22nd Floor
New York, New York 10010
Tel. (212) 849-7000
steigolson@quinnemanuel.com

Michelle Schmit
191 N. Wacker Drive, Suite 2700
Chicago, Illinois 60606
Tel. (312) 705-7400
michelleschmit@quinnemanuel.com

Attorneys for Plaintiffs-Counterclaim Defendants IQVIA Inc. and IMS Software Services, Ltd.